9110-9P P

DEPARTMENT OF HOMELAND SECURITY

The Department of Homeland Security, Stakeholder Engagement & Cyber Infrastructure Resilience Division (SECIR)

AGENCY: National Protection and Programs Directorate (NPPD), Department of Homeland Security (DHS).

ACTION: 30-day notice and request for comments; New Information Collection Request: 1670-NEW.

SUMMARY: The DHS NPPD Office of Cybersecurity and Communications (CS&C), SECIR, will submit the following information collection request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995. DHS previously published this ICR in the *Federal Register* on Tuesday, July 18, 2017 at 82 FR 32859 for a 60-day public comment period. Ten comments from two commenters were received by DHS. The purpose of this notice is to allow an additional 30 days for public comments.

DATES: Comments are encouraged and will be accepted until ***[INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].*** This process is conducted in accordance with 5 CFR part 1320.

ADDRESS: Interested persons are invited to submit written

comments on the proposed information collection to the Office of Information and Regulatory Affairs, OMB. You may send comments, identified by the words "Department of Homeland Security" and "OMB Control Number 1670-NEW (IT Sector Survey)", by:

- E-mail: dhsdeskofficer@omb.eop.gov. Include "Department of Homeland Security" and "OMB Control Number 1670-NEW (IT Sector Survey)" in the subject line of the message.

Instructions: Comments submitted in response to this notice may be made available to the public through relevant websites. For this reason, please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. If you send an e-mail comment, your e-mail address will be automatically captured and included as part of the comment that is placed in the public docket and made available on the Internet. Please note that responses to this public comment request containing any routine notice about the confidentiality of the communication will be treated as public comments that may be made available to the public notwithstanding the inclusion of the routine notice.

FOR FURTHER INFORMATION CONTACT: For specific questions related to collection activities, please contact Reggie

McKinney at 703-705-6277 or at reggie.mckinney@hq.dhs.gov.

SUPPLEMENTARY INFORMATION: Section 227 of the Homeland Security Act of 2002 authorizes the National Cybersecurity and Communications Integration Center (NCCIC) within NPPD as a "Federal civilian interface for the multi-directional and cross-sector sharing of information related to . . . cybersecurity risks." 6 U.S.C. 148(c)(1). This authority applies to Federal and non-Federal entities, including the private sector, small and medium businesses, sectors of critical infrastructure, and information sharing organizations. This provision includes the authority to receive, analyze and disseminate information about cybersecurity risks and incidents and to provide guidance, assessments, incident response support, and other technical assistance upon request and codifies NPPD's coordinating role among Federal and non-Federal entities. 6 U.S.C. 148.

As part of its information sharing responsibilities with non-Federal entities, the National Defense Authorization Act For Fiscal Year 2017 (NDAA) amended the Homeland Security Act to authorize the Department to specifically focus on small businesses. See Pub. L. 114-328 (2016). Specifically, the NDAA authorizes NPPD, through the Secretary, to "leverage small business development centers to provide assistance to small business

concerns by disseminating information on cyber threat indicators, defense measures, cybersecurity risks, incidents, analyses, and warnings to help small business concerns in developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees." See 6 U.S.C. 148(l)(1); see also 15 U.S.C. 648(a)(8)(A) (similarly authorizing DHS "and any other Federal department or agency in coordination with the Department of Homeland Security" to "leverage small business concerns by disseminating information relating to cybersecurity risks and other homeland security matters to help small business concerns in developing or enhancing cybersecurity infrastructure, awareness of cyber threat indicators, and cyber training programs for employees").

Consistent with these authorities, E.O. 13636 directs the Department to increase its cybersecurity information sharing efforts with the private sector and consult on and promote the National Institute of Standards and Technology (NIST) Cybersecurity Framework. To facilitate the Department's promotion of the NIST Cybersecurity Framework, the E.O. directs the Secretary to establish a voluntary program to support the adoption of the Framework in coordination with Sector Specific Agencies, which in turn

"shall coordinate with Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments." E.O. 13636, 78 FR 11739 (2013).

Accordingly, the Information Technology (IT) Sector, represented by industry via the IT Sector Coordinating Council (SCC) and by government via the IT Government Coordinating Council (GCC), established the IT Sector Small and Midsized Business (SMB) Cybersecurity Best Practices Working Group ("Working Group") to develop best practices for implementing the NIST Cybersecurity Framework in the SMB community. The Working Group, which consists of industry and government representatives, developed the SMB Cybersecurity Survey to determine return on investment (ROI) metrics for NIST Cybersecurity Framework adoption among SMB stakeholders. This process will assess the effectiveness of the NIST Cybersecurity Framework. This process will also establish a baseline for ROI metrics, which have not previously existed in the SMB community. The IT Sector-Specific Agency (SSA), headquartered in DHS NPPD CS&C, is supporting the Working Group's survey development.

DHS is not administering, controlling or soliciting the collection of the information via the survey. The IT SCC will administer the survey and anonymize the data, which will then be sent to DHS for analysis. As part of the survey process, the IT SCC will collect point of contact (POC) information but will not include that information on the anonymized dataset they submit to DHS. As specified in more detail below, the IT SCC will not only anonymize the data but will also remove any personally identifiable information (PII) from the data prior to transmitting to DHS. DHS will aid with the statistical analysis where needed, but would not be working with the individual responses to the questionnaire.

The questionnaire will be distributed to SMBs and is a two-part survey. Questions 1-11 of the survey are for an organization's leadership, as these questions pertain to high level information about the company (core function, number of employees, etc.). The remaining questions are intended for the Chief Information Security Officer (CISO) or appropriate IT staff, as these questions are technical and ask about the IT security of the company.

As identified above, once the survey is administered by the private sector partners of the IT SCC to the member organizations, the private sector partners of the IT SCC

will compile the collected raw inputs and will a) assign unique random identifiers to each of the responses, b) scrub any PII from the microdata, c) conduct quality assurance against the raw input. These processing steps (a-c) will be implemented PRIOR to transmitting the resulting dataset to DHS for statistical analysis. This survey represents a new collection.

DHS will use anonymized data to conduct their analysis. The intent is for DHS to only receive derivative products – anonymized micro-dataset to come up with the summary statistics, or aggregated summary results. The analysis will determine ROI information for NIST Cybersecurity Framework adoption in the SMB community. The results of this analysis will be available to the SMB community to develop best practices on how to use the Cybersecurity Framework for business protection and risk management.

OMB is particularly interested in comments that:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of

the burden of the proposed collection of information, including the validity of the methodology and assumptions used;

3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

Title of Collection: The Department of Homeland Security, Stakeholder Engagement & Cyber Infrastructure Resilience Division

OMB Control Number: 1670-NEW

Frequency: Once every five years

Affected Public: Private sector, Small & Midsize Businesses

Number of Respondents: 1,000 annually

Estimated Time per Respondent: 30 minutes

Total Burden Hours: 500 annual burden hours

Total Burden Cost (capital/startup): $0

Total Recordkeeping Burden: $0

Total Burden Cost (operating/maintaining): $0

David Epperson,
Chief Information Officer.
[FR Doc. 2017-27114 Filed: 12/15/2017 8:45 am; Publication Date: 12/18/2017]